ISO/IEC JTC 1/SC 27 N 2429

ISO/IEC JTC 1/SC 27/WG 3 N 489

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE:	Dispositions of Comments
TITLE:	Dispositions of comments on ISO/IEC Working Draft 15292 (SC 27 N 2335) Information technology – Security techniques - Protection profiles registration procedures
SOURCE:	19th SC 27/WG 3 meeting
DATE:	1999-10-08
PROJECT:	1.27.20
STATUS:	Output document of the editing session for ISO/IEC WD 15292 (SC 27 N 2335) held during the 19th SC 27/WG 3 meeting in Columbia, Maryland, USA, October 4 – 8, 1999. This document was available at the above-mentioned meeting. It is being circulated for information.
ACTION:	FYI
DUE DATE:	
DISTRIBUTION:	P, O and L-Members W. Fumy, SC 27 Chairman M. De Soete, T. Humphreys, M. Ohlin, WG-Conveners
MEDIUM:	Server
NO. OF PAGES:	8

Secretariat ISO/IEC JTC 1/SC 27 -
DIN Deutsches Institut für Normung e.V., 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: passia@ni.din.de;
HTTP://www.din.de/ni/sc27

ISO/IEC JTC 1/SC 27 N 2429

ISO/IEC JTC 1/SC 27/WG 3 N 489

ISO - International Organisation for Standardisation
IEC - International Electrotechnical Commission

JTC 1 - "Information Technology"
SC 27 - "Security Techniques"
WG 3 - "Security Evaluation Criteria"

TITLE: Disposition of Comments on WD 15292, Information technology – Security techniques – Protection profile registration procedures

SOURCE: ISO/IEC JTC 1/SC 27/WG 3 meeting, Colombia

DATE: 1999-10-08

PROJECT: JTC 1.27.20

STATUS: For distribution within JTC 1/SC27

Disposition of Comments for Project JTC1.27.20.

Comments were received on the Fourth WD for Protection Profile Registration Procedures (SC 27 N2335) from several National Bodies (see SC 27 N2384) and from ECMA (see SC27 N2389). These are answered below.

The Project Editor thanks these National Bodies and the Liaison Organisation for their continued diligent work in reviewing these drafts.

Attachment 1 to SC 27 N2384 – Canadian NB Comments

T1/2. Define period of time for action. Comment accepted and will be implemented.

T3. More than one pass statement or certificate? Currently, the sponsor is permitted to submit one statement or certificate for a register entry. If this statement or certificate expires or is withdrawn, the WD procedures as written permit the sponsor to submit a replacement statement or certificate immediately.

T4. Certificate withdrawn but pass statement stands? The WD procedures as written do permit the sponsor to submit the evaluation pass statement instead. See response to T3 above.

T5. Permit multiple certificate or pass statements in entries. Not accepted. Current procedures seem to satisfy the actual Canadian concerns – see responses to T3/4 above.

Attachment 2 to SC 27 N2384 – Danish NB Comments

This editorial correction is accepted and will be implemented.

Attachment 3 to SC 27 N2384 – French NB Comments

1. ISO/IEC Guide 58:1993 is entitled ”Calibration and testing laboratory accreditation systems – General requirements for operation and recognition”. The Project Editor will check that this is the correct ISO Guide to reference for this definition.

2. Certification status. Comment not accepted. The CC mutual recognition arrangement has no official ISO/IEC status. Until ISO/IEC recognise one or more relevant certification bodies or evaluation schemes as having an official status, all will be accepted.

3. ”Evaluator” not defined. Comment accepted. The definition will be reworded.

4. Re-introduce country of origin in EI label. Comment not accepted. In previous WDs, this field referred to the country of registration, not of origin. Also, for multi-national organisations, the country of origin might be misleading or meaningless.

5. EI title length. Comment accepted. This problem will be resolved by replacing the EI title with an overview description, without any maximum length. See US NB comments.

6. Mandate electronic copy of PP or package specification. Comment accepted. This requirement will be added.

7. What is incomprehensible information? This term is taken from the JTC1 regulations. It is intended to protect the RA from having to process applications that are too poorly prepared to be understood.

8. Who decides that a defect requires more than a resolution note? As worded, it is decided by the entry sponsor. Thus there would be no competition. It is believed that this reminder of an alternative solution to a defect problem is helpful. Therefore the note will be retained.

9. What is the ”Technical Specification”?. The term ”Technical Specification” is currently used with two different meanings in the WD. This is an editorial problem and will be resolved.

10. Two Years for SC Appeal. Comment not accepted. As the SC only meets once per year, and might need to consult NBs in reaching an appeal decision, two years is required to cover the case where an appeal is lodged, perhaps deliberately, just before an SC meeting so that there is not time to obtain proper NB views prior to the meeting.

Attachment 4 to SC 27 N2384 – German NB Comments

(No comments)

Attachment 5 to SC 27 N2384 – Japanese NB Comments

1. Make important elements of entry application in English only. Comment not accepted. Paragraph 5 requires these elements to be submitted in English, except by mutual agreement between the applicant and the RA. It seems unreasonable that, for example, an RA in France must not accept these declarations in French from a French-speaking applicant.

2. Declaration that the specification does not contain confidential information. Comment accepted, this requirement should be stated in Clause 13. Clause 13 will be reworded accordingly.

3. Identification of missing sections within incomplete entries. Comment accepted. A requirement will be added that missing sections must be marked in English, regardless of the language used to specify the technical content of the entry.

Attachment 6 to SC 27 N2384 – US NB Comments

1. Editorial correction – reference to ”EI” will be removed.

2. Editorial correction – comment accepted.

3. Difference between sponsor and applicant. The concept of ”applicant” comes directly from the JTC1 regulations and will therefore be retained. There is always a clean distinction between the two terms, except in clause 15. Clause 15 refers to both sponsors and applicants and is thus confusing. This problem will be resolved by rewording the clause.

4. This editors note will be removed in the next draft. It was present to explain why a request from another NB to use only definitions from established standards could not be implemented.

5. Technical Specification Clause. Following JTC1 regulations, a clause is required to specify the naming domain for registration. Clause 5 performs the purpose. It will be retitled to make its scope clearer and eliminate any conflict with later use of the term ”technical specification.” However, clause 5 should not define register entry or application contents – that is done in clauses 14 and 8 respectively. It is accepted that an overview, as defined for PPs in IS 15408-1 clause B.2.2b, should be part of the register entry. This requirement will be added to Clause 14. It is accepted that having the technical specification of a PP as the PP itself is strained. These references will be reworded.

6. Unique identifier problems. Comment and proposed solution accepted.

7. EI title length limit. It is accepted that the limit is arbitrary. However, another NB comment has been accepted that an overview of the register entry should be provided. In consequence, the EI title field will be withdrawn.

8. Register entry criteria. These are defined in subclause 9.2. A reference will be added here.

9. Language issues. Clause 14 (publication) will be clarified to make clear that the register is published in English.

10. Content of register entries. This is a Clause 14 issue. However, the intent is that both www and printed formats will contain at a minimum the mandated contents given in Clause 14. The RA may offer additional information if they wish.

11. Conflict with Clause 14 over language. The Editor believes that there is no conflict, and the current words are correct, since the RA may maintain several copies in different languages, although the mandated duty is to maintain a copy in English.

12. Language of correspondence. It seems unreasonable that correspondence between (for example) an RA in a French-speaking country and an applicant in that country must be in English (other than providing register information that must be in English). However, it is accepted that the current draft has caused confusion. The Editor will draft an additional clause or subclause on the issue of language.

13. Query sponsors of superseded entries. Comment accepted. However, will be addressed within requirements of clause 9.2.

14. Reference to other PPs etc. This requirement was introduced in response to a request from another NB to explicitly permit or prohibit such references. It is considered that permitting such references would significantly complicate the standard, for example in dealing with references to un-registered PPs or packages.

15. Conflict over use of ”confidential”. Comment and proposed resolution accepted.

16. Confirmation letter fraud. Comment accepted. The consistent approach would be to write to the sponsors of replaced entries on the same terms as evaluators or certifiers. This will be adopted.

17. Note on replacement sponsors. Comment and proposed solution accepted.

18. Language of submission issues. The need to revise and clarify this paragraph is accepted. The proposed solution of 18.3 will be adopted in this revision.

19. English language versions. See response to comment 18.

20. Overkill. Comment and proposed solution accepted.

21. How to ensure all required sections are present. There is a non-mandatory structure given in IS 15408-1 Annex B. This structure will be mandated for register applications.

22. Non-responding organisations. This comment is not accepted. There may be changes of address etc. causing non-response, as well as bogus information. The applicant should be given a chance to sort things out.

23. Cut automatic ”obsolescent” status for replaced/related entries. Comment and proposed solution accepted.

24. Missing or incomplete information. Comment accepted; however the best way to implement related changes may not be as proposed. See related Japanese comment.

25. One month to reply or out. ”No fault” problems can be handled by the appeals procedure. No change required.

26. Gratuitous defect reports. Re-evaluation is only required on three-yearly review. If defects have been reported, it seems wrong that evaluated status is maintained on re-registration. Current position seems to be the best trade-off between cost and confidence.

27. Recording defect reports. Comment partially accepted. A defect report should be recorded unless retracted during the resolution period – see response to 28. As sponsor specifies entry content, it seems best for them to describe defects as well.

28. Non-response action. See responses to 25 and 27.

29. Responsibilities. This comment is not accepted – see response to 27.

30. The comment that ”in writing” is not defined is accepted. The paragraph will be reworded. For information, JTC1 regulations now treat e-mail as equivalent to letter or fax. The history record comment is not accepted. JTC1 regulations required the first and current owner details to be recorded, and this currently required. Requiring intermediate owners to be recorded seems excessive as a mandatory requirement. If you disagree, please suggest a scenario where the extra information would be helpful.

31. Add certificate to 11.4 para 3 - Comment not accepted. In fact, what you are asking either organisation to confirm relates to the evaluation pass statement – it is this document that must match the submitted specification. Certificates merely authenticate pass statements. Improve wording – this comment and proposed solution accepted.

32. Database organisation. This comment is a recommendation to an RA appointed to operate this standard, not a comment on the WD.

33. Language issues. This comment is accepted. A new clause or subclause will be added to resolve issues of language.

34. Level of format detail. Comment not accepted. As required by ISO regulations, this Standard should normally only define what information is to be recorded (requirements) not how it is recorded (implementation). Clause 5 gives

implementation detail in order to ensure that every registered PP or package is given a unique entry identifier. This is expressly required by the JTC1 regulations for RAs.

35. Reference to ”Technical Specification”. Comment accepted. Ambiguity will be removed.

36. Multiple certifications. Comment not accepted. Lists of authorities recommending use of a PP or package is distinct from certification and registration and beyond the scope of this register. Multiple certification does not impact the status of an entry and is therefore not required as mandated content. Replacement of the registered certificate is already permitted – see response to Canadian comment T3.

37. Defect notes and resolutions. Comment and proposed solution accepted.

38. Incorporate overview. Comment accepted.

39. Mandatory English translation of PP or package definitions. Comment not accepted. Other, non-English speaking, NBs have advised of a need to register PPs or packages for which no English translation is available.

40. Awkward wording. Comment and proposed solution accepted.

41. Dispute resolution. The RA cannot be expected to resolve disputes concerning defect reports as it is not required to have any technical understanding of the content of register entries. All technical issues must be resolved by the entry sponsor. The defect reporter has no subsequent recourse.

42. SC Appeals. Since the SC meets only once per year, a long cycle is needed. See response to French comment 10. Two years is a short time in standards!

SC 27 N2389 – ECMA Comments

1. Invalid defect reports. It is considered that information, once recorded, should not be removed – a correction can be appended by the entry sponsor. See response to US NB comment 27.

2. Reversal of obsolescent status caused by e.g. accidentally delayed reply. ”No fault” problems can be handled by the appeals procedure. See response to US NB comment 25.